# SPYWOLF

## Security Audit Report

TrueFund.
SMART INVESTMENTS

Completed on
**June 25, 2023**

# OVERVIEW

This audit has been prepared for **TrueFund** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

*The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal*

- SPYWOLF Team -

# TABLE OF CONTENTS


## PROJECT DESCRIPTION

**According to their whitepaper:**

True fund is staking contract where you invest any amount into TrueFund and start earning 1.5% of this amount every day.
Your funds gradually return to you, and after several days when your Initial Investment is fully returned, you start making profits.
The period or making profits is unlimited: you can double or triple your Initial Investment by claiming your 1.5% Daily Reward.
It is pretty similar to how ordinary banks work but smarter, fair and generous.

**Release Date:** Launched at May 27th, 2023

**Category:** Staking

# CONTRACT INFO

Token Name
N/A

Symbol
N/A

Contract Address
0x24303F9A288055181fF62A57ae719770087846C2

Network
Binance Smart Chain

Language
Solidity

Deployment Date
May 13, 2023

Verified?
Yes

Total Supply
N/A

Status
Launched

# TAXES

Buy Tax
**10%**

Sell Tax
**10%**

# Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

**Blockchain security tools used:**

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

# TOKEN TRANSFERS STATS

| | |
|---|---|
| **Transfer Count** | N/A |
| **Uniq Senders** | N/A |
| **Uniq Receivers** | N/A |
| **Total Amount** | N/A |
| **Median Transfer Amount** | N/A |
| **Average Transfer Amount** | N/A |
| **First transfer date** | N/A |
| **Last transfer date** | N/A |
| **Days token transferred** | N/A |

# SMART CONTRACT STATS

| | |
|---|---|
| **Calls Count** | 2857 |
| **External calls** | 2857 |
| **Internal calls** | 0 |
| **Transactions count** | 2857 |
| **Uniq Callers** | 414 |
| **Days contract called** | 8 |
| **Last transaction time** | 2023-06-23 16:30:52 UTC |
| **Created** | 2023-06-16 00:05:45 UTC |
| **Create TX** | 0x0dd73aebf8c2ee4f3bd0f8cbd7c6abc62bad7094ad2e432088782b2187783663 |
| **Creator** | 0x84555cf70ce4bcdb97f201d150a9b1ca17ba2384 |

# VULNERABILITY CHECK

| | |
|---|---|
| Design Logic | Passed |
| Compiler warnings. | Passed |
| Private user data leaks | Passed |
| Timestamp dependence | Passed |
| Integer overflow and underflow | Passed |
| Race conditions and reentrancy. Cross-function race conditions | Passed |
| Possible delays in data delivery | Passed |
| Oracle calls | Passed |
| Front running | Passed |
| DoS with Revert | Passed |
| DoS with block gas limit | Passed |
| Methods execution permissions | Passed |
| Economy model | Passed |
| Impact of the exchange rate on the logic | Passed |
| Malicious Event log | Passed |
| Scoping and declarations | Passed |
| Uninitialized storage pointers | Passed |
| Arithmetic accuracy | Passed |
| Cross-function race conditions | Passed |
| Safe Zeppelin module | Passed |
| Fallback function security | Passed |

# THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

## High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## Low Risk

Issues on this level are minor details and warning that can remain unfixed.

## Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

# FOUND THREATS

## ⚠ High Risk

No high risk-level threats found in this contract.

## ⚠ Medium Risk

No medium risk-level threats found in this contract.

## ⚠ Low Risk

No low risk-level threats found in this contract.

# Informational

Owner can transfer funds from the Insurance contract to the TrueFund contract.

```
function pullInsurance(uint _amount) public OnlyOwner {

    _insurancePull( Flags.INS_ADMIN, _amount );
}

function _insurancePull(Flags _flag, uint _amountRequested) private {

    uint amountFunded = ITrueFundInsurance(INSURANCE).fundProject( _amountRequested );

    HT_INS_RECV_AGG += amountFunded;

    emit event_insurancePull(_flag, _amountRequested, amountFunded);
}
```

# Informational

From each new investment, 10% of the amount goes to contract's owner and 1% of the amount goes into insurance contract.

```
uint16 constant                 FEE_INVEST =            100;
uint constant                   INS_PER_INVEST =        10;

function invest(uint _amount, address _upline) external {
.....................
TOKEN.safeTransfer(OWNER, _per(_amount, FEE_INVEST) );
_insuranceFill( _per(_amount, INS_PER_INVEST), Flags.INVEST );
.....................
}

function _per(uint _amount, uint _percent) private pure returns(uint) {
    return (_amount * _percent) / 1000;
}


function _insuranceFill(uint _amount, Flags _flag) private {

    TOKEN.safeTransfer( INSURANCE, _amount );

    HT_INS_SENT_AGG += _amount;

    if(_flag == Flags.INVEST)   HT_INS_SENT[0] += _amount; else
    if(_flag == Flags.COMPOUND) HT_INS_SENT[1] += _amount; else
    if(_flag == Flags.WITHDRAW) HT_INS_SENT[2] += _amount; else
    if(_flag == Flags.UNSTAKE)  HT_INS_SENT[3] += _amount;
}
```

# Informational

If withdrawn amount is lower than 25% of current's contract total busd amount, 10% tax will be deducted from user withdraw and sent to the insurance fund contract.

```
uint constant                   INS_PER_WITHDRAW =      100;

function withdraw() external {
bool triggered = _insuranceTrigger(totalRewards);

if(!triggered) _insuranceFill( _per(totalRewards, INS_PER_WITHDRAW), Flags.WITHDRAW );
.....................
}

function _insuranceTrigger(uint _amount) private returns(bool) {

    uint balance = TOKEN.balanceOf(address(this));

    if(balance == 0) {

        _insurancePull( Flags.INS_TRIGGER_ZERO, TOKEN.balanceOf(INSURANCE) );
        return true;
    }

    if(_amount * 1000 / balance >= INS_PER_TRIGGER) {

        _insurancePull( Flags.INS_TRIGGER_HEAVY, _amount );
        return true;
    }

    uint avg = _avgBalance();
    if(avg > 0) {
        if(balance * 1000 / avg <= 1000-INS_PER_TRIGGER) {

            _insurancePull( Flags.INS_TRIGGER_AVG, avg - balance );
            return true;
        }
    }

    return false;
}
```

# Informational

Users can earn 1.5% per day from their total investment. There is rewards cutoff period of 24 hours - unclaimed earnings for more than 24 hours will count as earnings for 24 hours.
Example - If user staked, and did not claimed their rewards for period of 18 hours, user will receive reward for 18 hours.
Example - If user staked, and did not claimed their rewards for period of 1 day (24 hours), user will receive reward for 1 day (24 hours).
Example - If user staked, and did not claimed their rewards for period of 3 days, user will receive reward for 1 day (24 hours).

```
function withdraw() external {

    require( _isUser(msg.sender), 'Invalid user');
    User storage user = USERS[msg.sender];
    _encashEarnings(msg.sender);
    ....................................

}


function _min(uint num1, uint num2) private pure returns(uint) {
    return num1 < num2 ? num1 : num2;
}

function _encashEarnings(address _user) private {
    User storage user = USERS[_user];
    (uint timeFull, uint timeEarn, uint amtFull, uint amtEarn, /*daily*/) = _calcEarnings(_user);
    user.checkpoint = block.timestamp;
    user.earnReward += amtEarn;
    user.ht_earned += amtEarn;
    HT_EARNED += amtEarn;

    HT_TIMER_AMT += timeFull - timeEarn;
    HT_TIMER_CNT++;

    emit event_encashEarnings(_user, timeFull, timeEarn, amtFull, amtEarn);
}

function _calcEarnings(address _user) public view returns(uint _timeFull, uint _timeEarn, uint _amtFull, uint _amtEarn, uint _daily) {

    User storage user = USERS[_user];

    _timeFull = user.checkpoint > 0 ? block.timestamp - user.checkpoint : 0;
    _timeEarn = _min( _timeFull , EARNINGS_CUTOFF );

    _amtFull = (user.invested * _timeFull * DAILY_ROI) / 86400000;
    _amtEarn = (user.invested * _timeEarn * DAILY_ROI) / 86400000;
    _daily = (user.invested * DAILY_ROI) / 1000;

}
```

# Informational

There is referral rewards system implemented with up to 10% rewards per deposit.
Referral line is up to 3 referrals which will receive 6%, 3%, 1% of the deposited amount respectively (total 10% of amount deposited).

```
uint16[REF_LVLS] public         REF_PERCENTAGES =       [60, 30, 10];

function invest(uint _amount, address _upline) external {
.....................
_refPayout(msg.sender, _amount);
.....................
}

function _per(uint _amount, uint _percent) private pure returns(uint) {
    return (_amount * _percent) / 1000;
}

function _refPayout(address _user, uint _amount) private {

    address upline = USERS[_user].upline;

    for(uint8 i = 0; i < REF_LVLS; i++) {

        if(upline == address(0)) break;

        uint reward = _per( _amount, REF_PERCENTAGES[i] );

        User storage referrer = USERS[upline];

        referrer.refReward += reward;

        referrer.ht_refReward += reward;

        HT_REFREWARD += reward;

        _userHistory(referrer, Flags.REFPAYOUT, reward, 0, 0, _user, address(0) );

        emit event_refPayout(upline, _user, reward);

        upline = referrer.upline;
    }
}
```

RECOMMENDATIONS FOR

# GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

## True Fund

### GOOD PRACTICES FOUND

- ✔ The owner cannot stop or pause the contract

Staking contract.

TOKENOMICS

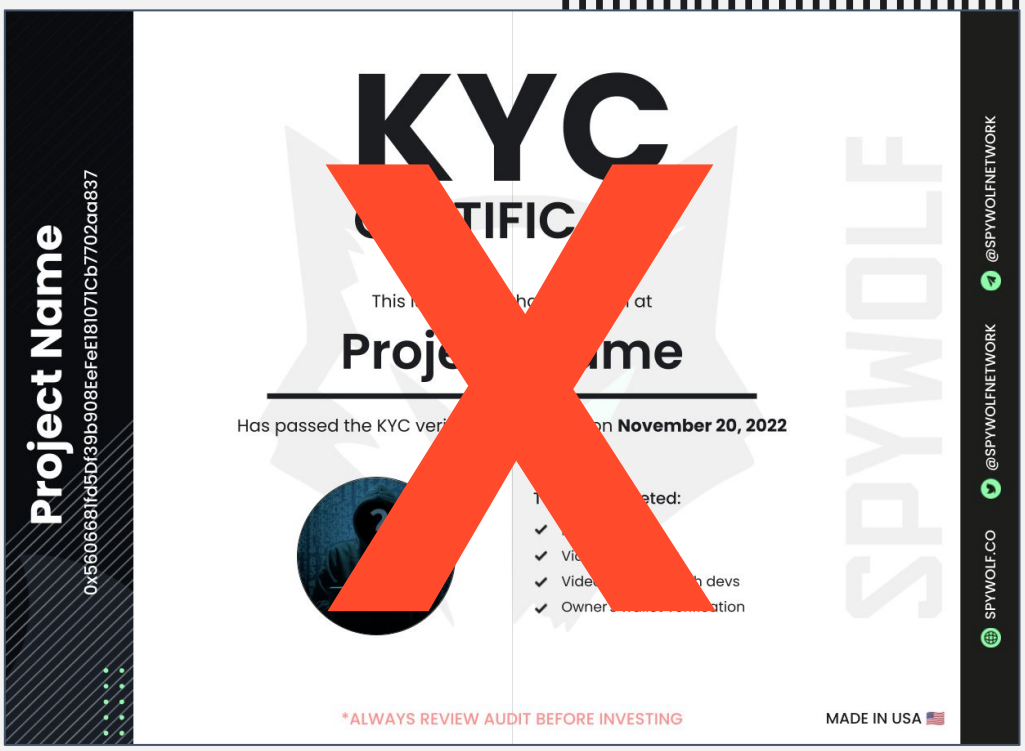
# THE TEAM

⚠️ The team is annonymous

## KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

## Website URL
https://truefund.app/

## Domain Registry
https://www.tldregistrarsolutions.com/

## Domain Expiration
2024-04-10

## Technical SEO Test
Passed

## Security Test
Passed. SSL certificate present

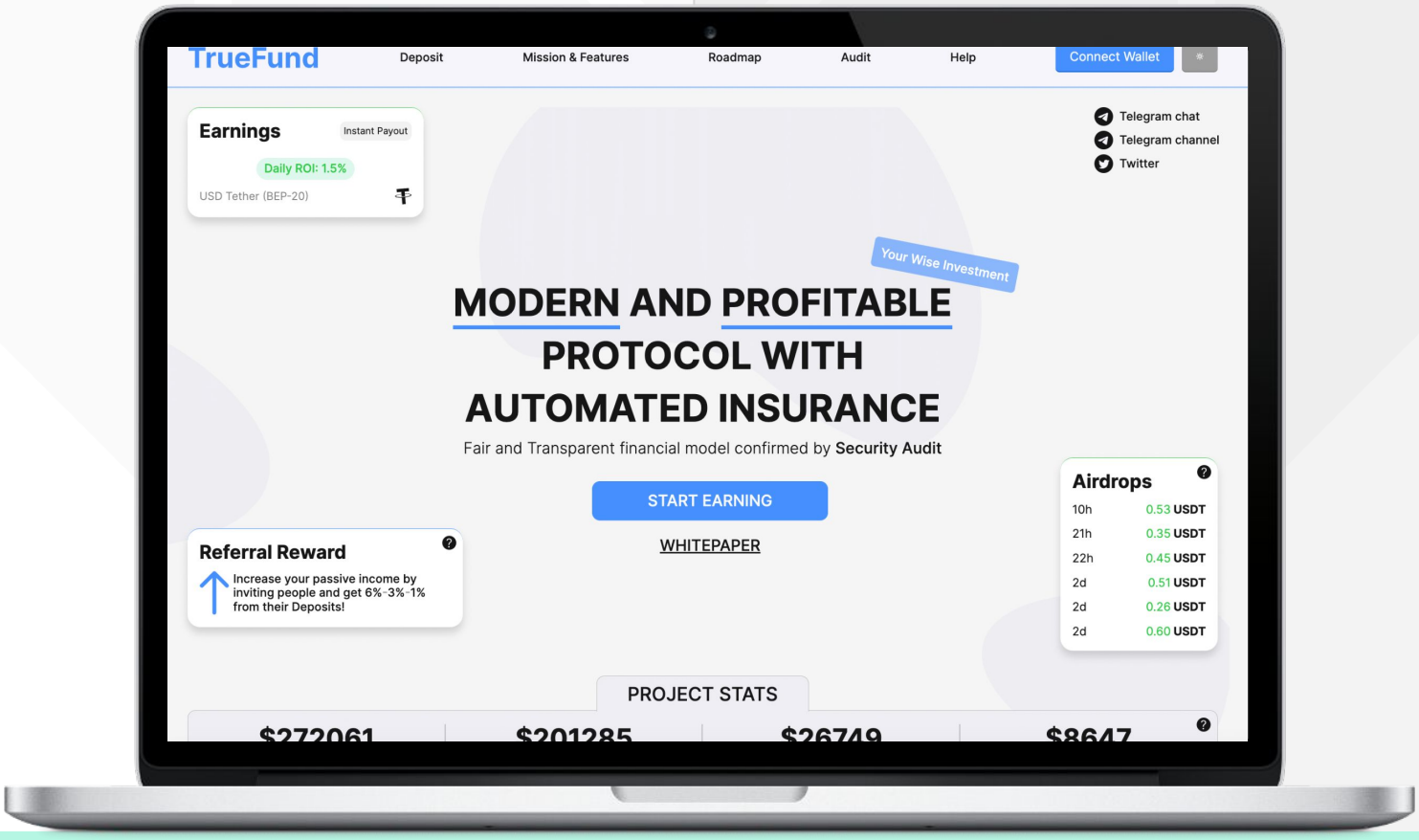
## Design
Very nice design with appropriate color scheme and graphics.

## Content
The information helps new investors understand what the product does right away. No grammar mistakes found .

## Whitepaper
Well written, explanatory.

## Roadmap
Yes, goals set without time frames.

## Mobile-friendly?
Yes



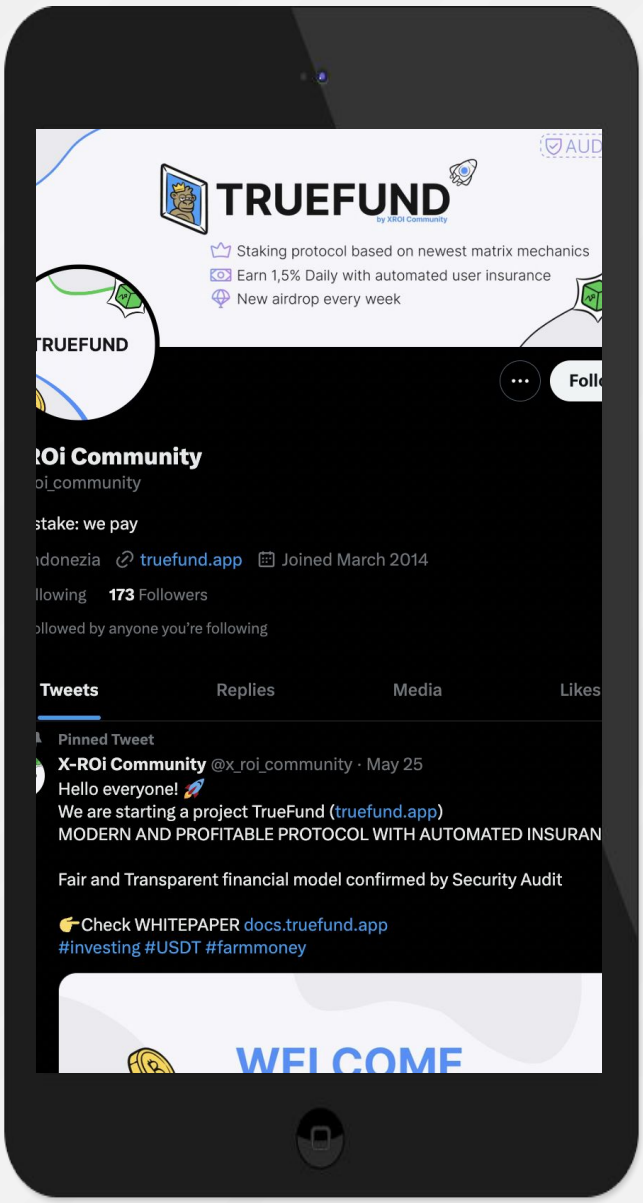

# truefund.app

# SOCIAL MEDIA

## & ONLINE PRESENCE

**ANALYSIS**

**Project's social media pages are active**




### Twitter

@x_roi_community

- 170 followers
- 3 total posts

### Discord

- Not available

### Telegram

@truefund_chat

- 860 members
- Active members
- Active mods

### Medium

- Not available

# SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

# ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

## FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

# Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

**DISCLAIMER:**
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.